# Smart Decision Making for Internal Attacks in Wireless Sensor Network

**Muhammad R Ahmed[†], Xu Huang[†] and Hongyan Cui[††]**

[†]Faculty of Information Sciences and Engineering, University of Canberra, Australia
[††]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, China

**Summary**
An information procuring and processing emerging technology Wireless Sensor Network (WSN) consists of low-cost and multifunctional resources constrain autonomous nodes. It communicates short distances through wireless links. It is open media and underpinned by an application driven technology for information gathering and processing. It can be used for many different applications range from military implementation in the battlefield, environmental monitoring, health sector as well as emergency response of surveillance. With its nature and application scenario WSN had drawn a great attention. It is known to be valuable to variety of attacks for the construction of nodes and distributed network infrastructure. In order to ensure its functionality especially in malicious environments, security mechanisms are essential. Malicious or internal attacker has gained prominence and poses the most challenging attacks to WSN. Even though several works have been done to secure WSN, but identification of abnormal behavior to detect internal attacks has not been given much attention. The conventional cryptographic technique does not give the appropriate security to save the network from internal attack. Without a fixed security infrastructure a WSN needs to find the internal attacks is a challenge as internal attacker behave like legitimate nodes. In this paper, we have proposed a new approach for detecting internal attack in two stages. In the first stage we will do the misbehavior judgment with Abnormal Behavior Identification Mechanism (ABIM) by using cosine similarity. Secondly, we use Dempster-Shafer theory (DST) of combined multiple evidences to identify the malicious or internal attacks in a WSN. The advantage of this method is it does not need the knowledge about the normal or malicious node in advance.

***Key words:***
*Wireless Sensor Network (WSN), internal attack, Abnormal Behavior Identification Mechanism (ABIM), Dempester Shafer Theory, Abnormal behavior*

## 1. Introduction

Significant improvement in wireless communication and electronics development in the last decade motivated to develop low power, low cost and multi-functional wireless devices. Wireless sensor networks are a new technology for collecting data with autonomous sensors [1]. It is first motivated by military applications such as battlefield surveillance, transportation monitoring, and sensing of nuclear, biological and chemical agents [2-5]. Recently, this technology became more popular because of its cost effectiveness and our daily life applications such as habitat monitoring [6], intelligent agriculture, and home automation [7]. It consists of large number of low cost, low power and multifunctional sensors embedded with short range wireless communication capability. The data is transmitted to the sink in an autonomous way which has high capacity of storage and analysis power. According to the applications the deployment strategy is decided [8]. When the environment is unknown or hostile such as remote harsh fields, disaster are as toxic environment the deployment usually done by scatter by a possible way, sometimes by small an aircraft. Thus the position of the sensor nodes may not be known in advance. In the post deployment the sensor nodes perform self-organization mechanism to set up the network by determining the neighbor and setting up the routing table by themselves in an autonomous way. A typical WSN shown in Figure 1.

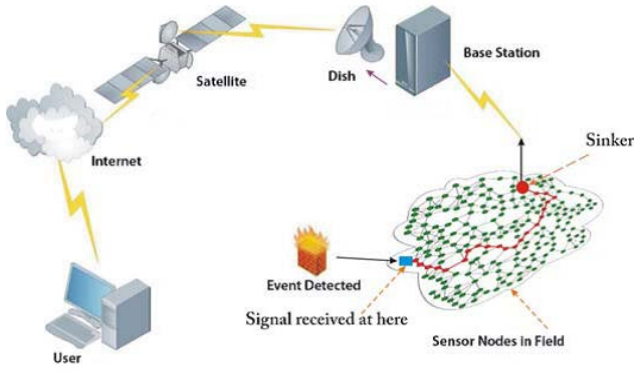


Figure 1. A typical WSN

Security provisioning is a critical requirement for any communication network. Security in the wireless sensor network is challenging and important task because of its characteristics that includes, open nature of wireless medium, unattended operation, limited energy, memory, computing power, communication bandwidth, and communication range. [9] So, it is more susceptible to the security attack compare to the traditional wired network as well as wireless ad hoc network.

Manuscript received December 5, 2012
Manuscript revised December 20, 2012

Although WSN shares many properties with Wireless ad hoc network and may require similar techniques such as routing protocols but in certain cases it directly prohibit using the protocols proposed in wireless ad hoc network. Thus, the characteristics and architecture differs as well. To demonstrate this issue, the dissimilarities between the WSN and wireless ad hoc network are summarized: [10]

• The number of sensor nodes (hundreds or thousands nodes) in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network.

• Sensor nodes are densely deployed, so multiple sensors can perform to measure the same or similar physical phenomenon.

• Sensor nodes are prone to failures because of battery exhaustion and hostile environment.

• The topology of a sensor network changes very frequently caused by node failure.

• Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to-point communications.

• Sensor nodes are limited in power, computational capacities, and memory.

• Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

The unique properties and characteristics of WSN need to be considered in order to secure the WSN. Many algorithms have developed for the secure functionality of WSN. Most of the work has focused on the pair wise key establishment, authentication access control and defense against attack. Most importantly those works mainly focused on the traditional cryptographic information, data authentication in order to build the relationship between the sensors. However, the unreliable communications through wireless channel made the communication technique vulnerable by allowing the sensor nodes to compromise and release the security information to the adversary [11]. The compromised entity of the network acts as a legitimate node. So it is easy for the adversary to perform the internal attacks. When internal attack occurs for a node, this node will behave abnormally such as tampering the massage from other member, dropping the data or broadcast excessive data.

So far, not much attention has been given to protect the network from the internal attack. In this paper, we have proposed two-stage mechanism to find the internal attack in a targeted WSN. In the initial stage we use the ABIM (cosine similarity method) to find the abnormally behaved or misbehaved node based on the message frequency with *k*-means algorithm [12]. In the second stage we used Dempester- Shafer Theory (DST) to make final decision about the targeted node. This algorithm observes neighbour nodes parameters to make the judgment based on the DST. DST has the feature of dealing with uncertainty [13]. It considers the observed data as hypothesis. It might be uncertain which hypothesis fits best. Therefore, DST makes it possible to model several single pieces of evidence within multi hypotheses relations [14]. In our proposed method the system does not need to have any prior knowledge of the pre-classified training data of the nodes.

The paper is organized as follows: section 2 is comprised of the overview of the related work followed by the Network assumptions and method in section 3. This section covers the details of internal attacker identification process. The efficiency of the framework is presented in Result section followed by conclusion section 5.

## 2. Internal Attacks in WSN

Simple sensor nodes are usually not well physically protected due to they are cheap and are always deployed in open or even in hostile environments where they can be easily captured and compromised, hence, an adversary can extract sensitive information, control the compromised nodes and let those nodes service for the attackers. The attacks are involved in corrupting network data or even disconnecting major part of the network.

Following our previous paper [8] the major internal attacks in WSN include Denial of Service (DoS) attacks, information and selective forwarding, Wormhole attack, node replication, Sybil attacks or black-grey-sink holes, and HELLO flooding. Etc..

Unlike traditional routing, where intermediate nodes just forward input packets, in network coding intermediate nodes actively mix or code input packets and forward the resulting coded packets. The very nature of packet mixing also subjects network coding systems to a severe security threat, knows as a pollution attack, where attackers inject corrupted packets into the network. Since intermediate nodes forward packets coded from their received packets, as long as least one of the input packets is corrupted, all output packets forwarded by the node will be corrupted. This will further affect other nodes and result in the epidemic propagation of the attack in the network. In [15], it addressed pollution attacks against network coding systems in wireless mesh networks.

## 3. Related work

Traditionally Internal attack detection by misbehavior has produced in the literature for peer to peer and ad hoc networks, but for WSN little work has been done. With the indication of misbehavior of the node we can find the internal attack in the network. So far, security using internal attack detection based on abnormal behavior or misbehavior not given much attention. Abnormal behavior (misbehavior) of the node has been proposed in different research but main focus was given on preventing and securing routing from attacks.

Intrusion detection in Wireless sensor network is studied in [16, 17], In [16] Zhang *et al*. proposed a scheme which is the first work on intrusion detection in wireless ad hoc networks. A new architecture is investigated for collaborative statistical anomaly detection which provides protection from attack on ad hoc routing. Silva *et al*. in [17] shows that an intrusion alarm is raised when number of failures exceeds a pre-defined threshold. This method the decision is made based on a simple summation of the rule whereas multiple rules have been defined.

To detect abnormal behavior Staddon *et al* [3] proposed to trace the failed nodes in sensor networks at the base station assuming that all the sensor measurement will be directed along the sinker based on the routing tree. In this work the sinker has the global view of the network topology and can identify the failed nodes through route update message and it is directional.

Watchdog like technique is proposed in [18], [19] and [20]. The purpose of the watchdog mechanism is to identify a malicious node by overhearing the communication of the next hop. This technique can detect the packet dropping attack by letting nodes listen to the next hope nodes broadcasting transmission. Normally, multiple watchdog work collaboratively in decision making and reputation system is necessary to provide the quality rating of the participants.

Karlof and Wagner discussed attacks at the network layer in [21] and mentioned altered or replayed routing information and selective forwarding, node replication, Sybil attacks or black-grey-sink holes, and HELLO flooding. Some papers discussed various attacks in term of network's resiliency, such as [15], they discussed how to keep WSN routing protocols as stateless as possible to avoid the proliferation of specific attacks and provide for a degree of random behaviour to prevent the adversary from determining which the best nodes to compromise are. They defined three items, namely (i) average delivery ratio, (ii) average degree of nodes, and (iii) average path length to describe the networks resiliency. Obviously, the more efficient and effective ways are needed.

Unlike traditional routing, where intermediate nodes just forward input packets, in network coding intermediate nodes actively mix or code input packets and forward the resulting coded packets. The very nature of packet mixing also subjects network coding systems to a severe security threat, knows as a pollution attack, where attackers inject corrupted packets into the network. Since intermediate nodes forward packets coded from their received packets, as long as least one of the input packets is corrupted, all output packets forwarded by the node will be corrupted. This will further affect other nodes and result in the epidemic propagation of the attack in the network. [22] addressed pollution attacks against network coding systems in wireless mesh networks. They proposed a lightweight scheme, DART that uses time-based authentication in combination with random liner transformations to defend against pollution attacks.

A few papers also address pollution attacks in internal flow coding systems use special crafted digital signatures [23-24] or hash functions [25-26]. Recently some papers discuss the preventing the internal attacks by related protocols [27-28].

Recently Game theory is commonly used to analyze wireless networks with selfish/attacker nodes. Reddy and Ma studied game theory based approach in [29-30], Reddy *et al*. approach in [29] using zero-sum game may find malicious sensor nodes in the forwarding path only. This method need to maintain a certain level of energy. The proposed method in [30] not only improves the security of WSNs, but also reduces the cost caused by monitoring sensor nodes and prolongs the lifecycle of each sensor node. However, the method does not consider the effects of the selfishness of the sensor nodes, which can discard normal packets or not transfer normal packets in WSNs.

Most of the existing related works are for ad hoc networks. With the differences in WSN and Wireless ad Hoc network the security mechanism for ad hoc network cannot protect WSN completely. Moreover, it is well know that most of existing mechanisms are based essentially on cryptographic primitives. In cryptographic approaches, the source uses cryptographic techniques to create and send additional verification information that allows nodes to verify the validity of coded packets. Polluted packets can then be filtered out by intermediate nodes. The proposed schemes rely on techniques such as homomorphic hash functions or homomorphic digital signatures. These schemes have high computational overhead, as each verification requires a large number of modular exponentiations. In addition, they require the verification information, such as hashes or signatures to be transmitted separately and reliably to all nodes in advance, which is normally difficult to achieve efficiently in wireless networks.

## 4. Network assumptions and Method

### 4.1 Assumptions

The system under consideration consists of an area of interest where region wise detection requirements are provided by the end user. We model the area of interest as a grid $\Omega$ of $N_x \times N_y$ points scenario. Sensors and channels are stationary after deployment of the network. Sensing nodes are responsible to collect and forward the monitored data around them to the sink. In order to detect the internal attack of WSN we use the DST mechanism. We will consider the system is synchronized.

In addition, for the temperature measurement, as a case study in this paper, we will consider that the sensor deployed area temperature vary from 8 degree to 14 degree in Celsius. Based on the Gaussian distribution within 2

sigma (the standard deviation of the Gaussian distribution), we will accept the temperatures. According to Holder *et al* [31], the choice of sigma value depends on the data set, 95.46% of the sensor data will fall within 2 standard deviation of the mean with 2 sigma consideration.

We will consider the temperature reading is normal or the node is behaving normally, if we find that the reading match with the sigma value and with the reading with the one hop neighbors and it is within the message frequency which is 0.1 Hz. If the outcome from ABIM is abnormal node we will do second stage implementation with DST.

Our temperature measurement WSN system is based on a single sinker with randomly distributed static node. We assume the neighbor node with one hop will observe the data of the suspected internal attacker. In order to observe, the physical parameter (Temperature) and transmission behavior (packet drop rate) is considered as independent events. The observation of the events becomes the pieces of evidences. In the decision making process with Dempster-Shafer Theory we will combine the independent pieces of evidences.

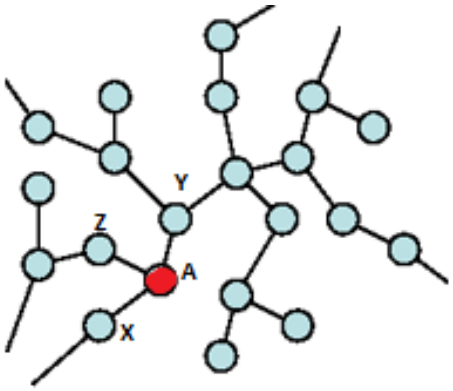


Figure 1: Three neighbor observing the attacker with one hop

Let's consider the above scenario described in Figure 1, neighbor nodes $X$ , $Y$ and $Z$ will observe the ABIM suspected abnormal node or internal attacker node $A$ for its temperature (T) and packet drop rate (PDR). In order to implement we need brief understanding of the theory. Both the theory and the concept of implementation is described in the section 4.

## 4.2 Abnormal Behaviour Identificaion Mechanism

In order to identify the misbehavior or abnormal behavior of the node we have designed ABIM that is sensitive to the abnormal event. In the conventional cryptographic way it is not possible to detect the internal attacker because of the unpredictable wireless channel. The unreliable channel makes it easy to compromise the node and establish untrustworthy relationship [32]. The attacker always behaves abnormally, so it is mandatory to identify the misbehaved node to secure the network.

WSN is densely deployed and continuously observe the phenomenon, this characteristics drive WSN node normally encounter the spatio-temporal correlation. In our research we considered the message generated from the nodes is similar for a defined period with the sampling rate if 0.1Hz (1 message per 10 second). Considering the limited storage of the sensor we store minimum information of the Message in *S*. The message $m_i$ is consists of the content of the representative message ( $\partial$ ) and frequency of the message ( $\alpha$ ). $m_i = \langle \partial_i, \alpha_i \rangle$ , The set of the message is shown in the equation (1)

$$S = \{m_1, m_2, m_3, .....m_n\} \tag{1}$$

It is the set that will store the latest message that is sent to the network recently. When a new message $m_{new}$ is sent it arrives at the cluster head which can be authenticated by the similarity function with *S*. The difference between the detected and average temperature is divergence. If we denote $D^i(m_{new})$ as the divergence between the new and the normal message we have the set as equation (2) for different cluster. [12]

$$D^i(m_{new}) = \{D^1(m_{new})D^2(m_{new}).....D^m(m_{new})\} \tag{2}$$

where,

$$D^i(m_{new}) = |m_m - m_{new}|$$

Based on equation (1) if the data is different from the content considering the Gaussian distribution of temperature and the threshold than it is new message. The threshold is defined as the mean of the data set. If $D^i(m_{new})$ is not within the threshold it is considered as new message. For further authentication we will use the cosine similarity with frequency consideration. If we consider new message frequency $\omega$ , the cosine similarity is in equation (3).

$$COSIM = \frac{\alpha.\omega}{\|\alpha\|\|\omega\|} \tag{3}$$

If the two frequencies are similar it is considered as normal message otherwise it is considered as false message and the node will be considered as abnormal node.

In this method the computation is simpler with smaller latency. The considered parameter for this process is supported by the resources constrained sensor nodes. [33]

Algorithm 1

I. Get $m_{new}$

For $i$ = 1 to $|M|$

If $MinTh \le D^i(m_{new}) \ge MaxTh$

printf "Good Node"

else go to II

II. for $i$ = 1 to $T$

Execute the equation (10)

If COSIM $i \le 0.6$

printf "the node is an internal attacker"

else

Go to step I

end

## 4.3 Dempester-shafer Theory

In DST, probability is replaced by an uncertainty interval bounded by belief and plausibility. Belief is the lower bound of the interval and represents supporting evidence. Plausibility is the upper bound of the interval and represents the non-refuting evidence [34]. In this reasoning system, all possible mutually exclusive hypothesis (or events) of the same kind are enumerated in the frame of discernment also known as universal discloser $\theta$. A basic belief assignment (BBA) or mass function is a function *m*: $2^{\theta} \rightarrow$ [0, 1], and it satisfies two following conditions

$$m(\phi) = 0 \tag{4}$$

$$\sum_{A \subseteq \theta} m(A_j) = 1 \tag{5}$$

In which $\phi$ is the empty set and a BBA that satisfy the condition $m(\phi) = 0$. The basic probability number can be translated as $m(A)$ because the portion of total belief assigned to hypothesis $A$, which reflects the evidences strength of support. The assignment of belief function maps each hypothesis $B$ to a value $bel(B)$ between 0 and 1. This defined as

$$bel(B) = \sum_{j:A_j \subseteq A} m(A_j) \tag{6}$$

The upper bound of the confidence interval is the plausibility function, which accounts for all the observations that do not rule out the given proposition. It maps each hypothesis *B* to a value $pls(B)$ between 0 and 1, can be defined as follows.

$$pls(B) = \sum_{j:A_j \cap B \neq \phi} m(A_j) \tag{7}$$

The plausibility function is a weight of evidence which is non-refuting to *B*. equation (8) shows the relation between belief and plausibility.

$$pls(B) = 1 - bel(\sim B) \tag{8}$$

The hypothesis not *B* is representing by ~*B*. The functions basic probability numbers, belief and plausibility are in one-to-one correspondence and by knowing one of them; the other two functions could be derived. [35] Figure 2 shows the graphical representation of the above defined measures belief and plausibility.

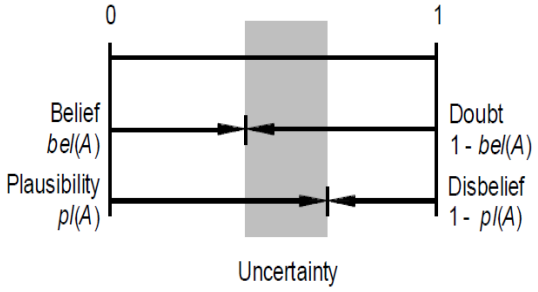


Figure 2. Measure of belief and plausibility

Assuming $m_1(A)$ and $m_2(A)$ are two basic probability number by two independent items of evidence means two independent neighbor node which act as observers in the same frame of discernment. The observations (the pieces of evidence) can be combined using Dempster's rule of combination (known as orthogonal sum) as in equation (9).

$$(m_1 \oplus m_2)(B) = \frac{\sum_{i,j:A_i \cap A_j = B} m_1(A_i)\, m_2(A_j)}{1 - \sum_{i,j:A_i \cap A_j = \phi} m_1(A_i)\, m_2(A_j)} \tag{9}$$

where $\oplus$ represents the Dempster's combination operator that combines two basic probability assignments or basic belief assignments (BBA) into the third [36]. To normalize the equation we consider *L* is a normalization constant defined by the equation (10), More than two belief function can be combined with pairwise in any order.

$$L = \frac{1}{K} \tag{10}$$

Where ,

$$K = 1 - \sum_{i,j:A_i \cap A_j = \phi} m_1(A_i)\, m_2(A_j)$$

The combination rule assigns the belief according to the degree of conflict between the evidences and assigns the remaining belief to the environment and not to common hypothesis. It makes possible to combine with most of their belief assigned to the disjoint hypothesis without the side effect of a counterintuitive behavior. Belief resembles the

certainty factors or evidences [37-38]. The conflict between two belief functions $bel_1$ and $bel_2$, denoted by the $Con(bel_1, bel_2)$ is given by the logarithm of normalization constant shown in equation (11)

$$Con(bel_1, bel_2) = \log(L) \quad (11)$$

The DST automatically incorporates the uncertainty coming from the conflicting evidences. Following the reference [38] we can come up with a Dempester-shafer combination, which can be given as in equation (12)

$$m(B) = (m_1 \oplus m_2)(B) = \frac{L \sum_{i,j:A_i \cap A_j = B} m_1(A_i)\, m_2(A_j)}{1 + \log(L)} \quad (12)$$

DST application in our system works by considering the independent event as temperature T and PDR as described in section 3. Our case the universal discloser or the set of local element can be observed by the one hop neighbor is $\theta = \{T, PDR\}$. Hence the power set becomes

$$2^{\theta} = \{\phi, \{T\}, \{PDR\}, \{unknown\}\}$$

Where,

$$\{unknown\} = \{T\} \cup \{PDR\}$$

In our specific case study and in simulation we have the imperial data for the T and PDR the basic probability assignments for the nodes $X$, $Y$ and $Z$ are as follows,

$m_T(X) = 0.7$ ; $m_T(Y) = 0.75$ ; $m_T(Z) = 0.65$ ; $m_T(U) = 0.1$

$m_{PDR}(X) = 0.75$ ; $m_{PDR}(Y) = 0.7$ ; $m_{PDR}(Z) = 0.75$

Implementing the DST as in equation (12) we can find the individual nodes observation about the suspected node $A$, based on the independent pieces of information or evidence.

$$m_{T,PDR}(X) = m_T(X) \oplus m_{PDR}(X)$$

$$m_{T,PDR}(Y) = m_T(Y) \oplus m_{PDR}(Y)$$

$$m_{T,PDR}(Z) = m_T(Z) \oplus m_{PDR}(Z)$$

From the above we have calculated one observation in which, we can see that the node $A$ is compromised with the probability of 0.61, 0.61 and 0.58 by the observation of node $X$, $Y$ and $Z$ respectively.

Algorithm 2

I. Get the view of the neighbor node view

Input: $m_T$, $m_{PDR}$, $\partial_T$, $\partial_{PDR}$

$m_T[\ ]$ \\ BPA assignment

$m_{PDR}[\ ]$ \\ BPA assignment

II. Execute the equation (9)

$m_{T,PDR}[\ ]$ \\

If $m(B) < 0.6$

Output result accepted

printf "the node is an internal attacker"

else

Go to step I

end

## 5. Result

Temperature measurement is considered in our experimental work with randomly deployed sensors. For the temperature range we have considered Gaussian distribution mean with 2 sigma similar to the approach taken by holder *el at* [31], even though in holder experiment he used 1 sigma for the constrain of data set but we assume we have sufficient data set to choose 2 sigma. In the data set we consider that the temperature vary from 8 degree to 14 degree centigrade. In the simulation environment the parameter we have set is shown as follows,

Table 1: Parameter

| Parameters | Values |
|---|---|
| Packet Size | 500 bytes |
| Initial Energy | 2 J |
| Cluster Radius | 50m |
| Regional Area | (0,0) to (500,500) |

In WSN sensor field, we have done the experiment with 20 sensors with the assumed temperature range of 8 to 14 degree centigrade. Based on the Gaussian distribution the mean and data threshold was calculated. In the DST implementation we have dove 100 different observations by the neighbor nodes. The experiment was done in the MATLAB environment. The abnormal was identified according to the methodology of ABIM. Figure (3) shows the sensor filed with 20 sensors with randomly distributed data the abnormal node shown in red (node 16). The value was set 29 degree to make node 16 as a suspected node for the simulation purpose.

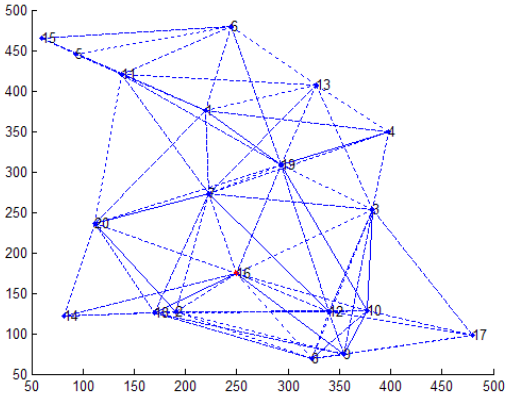

Figure 3. Sensor field

In this, ABIM checks the data with the nearest one hop neighbor and the average data of the network. If it finds that the suspected node data is not matching with one hop or with the average of the network, ABIM tells that the node is behaving abnormally. With the decision of ABIM we farther implement Dempester-shafer Theory (DST). Figure 4 describe the observation about the node *A*. it shows the observation by node *X*, *Y* and *Z*. from the figure it is clearly seen that three nodes observation gives the common result between 65 % to 70% that the node *A* is compromised or an internal attacker.

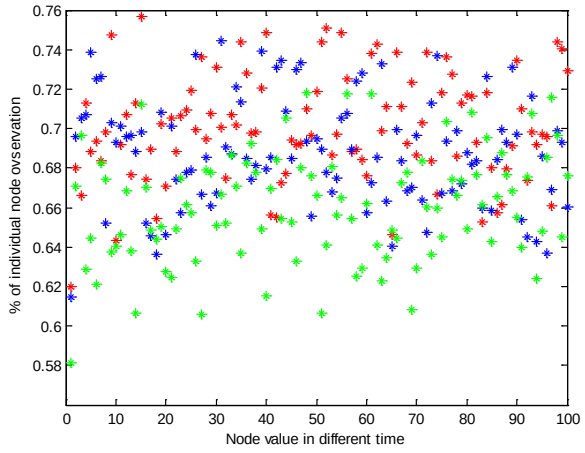


Figure 4. Observation of node A by X,Y,and Z

We have run 10 tests for Support Vector Machine (SVM) and our method in simulation with imperial data from the temperature measurement filed. We found that our method gives the higher accuracy compare to the SVM method.

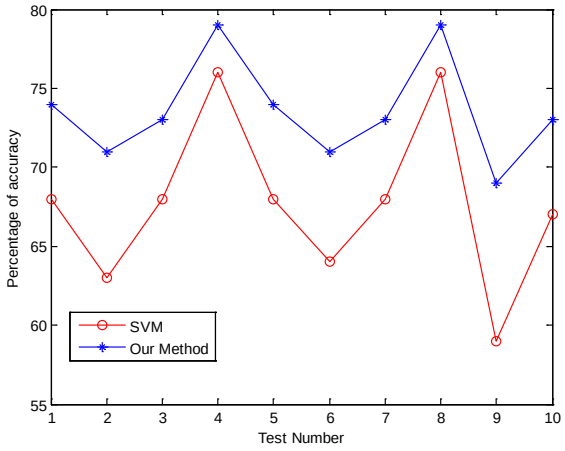


Figure 5. Accurecy of Detection

## 6. Conclusion

Internal Attack detection using abnormal behavior identification method (ABIM) by cosine similarity and Dempster-shafer theory (DST) is presented in this paper. Internal attacked node behavior always mismatch with the other neighbor nodes. So, misbehavior detection will lead to evaluate the internal attack of the in the WSN by DST implementation by evidential evaluation. The simulation result shows the detected abnormal node and evaluation done by DST with numerous observations.
In our future work we would like to implement the algorithm in the hardware level to test in real time environment.

### Acknowledgments

This project is supported by the Commonwealth of Australia under the Australia-China Science and Research Fund (ACSRF02541). One of authors would like to thank the work has been partly supported by the national Natural Science Foundation of China (Grant No. 61201153) the National 973 Program of China under Grant (No. 2012CB315805).

### References

[1] Huang X, Ahmed M, Sharma D, “Timing Control for Protecting from Internal Attacks in Wireless Sensor Networks”, IEEE, ICOIN 2012, Bali, Indonesia, February 2012.

[2] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, “Detection, classification, and tracking of targets”, IEEE Signal Processing Mag., vol. 19, pp. 17-29, Mar 2002.

[3] C. Meesookho, S. Narayanan and C. Raghavendra, “Collaborative classification applications in sensor networks”, Proc. of Second IEEE Multichannel and Sensor array signal processing workshop, Arlington, VA, 2002.

[4] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, B. Krogh, “An energy-efficient surveillance system using wireless sensor networks”, MobiSys'04, Boston, MA, 2004.

[5] B. Sinopoli, C. Sharp, L. Schenato, S. Shaffert, Sh. S. Sastry, “Distributed control applications within sensor networks”, Proc. Of the IEEE, August 2003.

[6] P. Sikka, P. Corke, P. Valencia, C. Crossman, D. Swain, and G. Bishop-Hurley, "Wireless ad hoc sensor and actuator networks on the farm," 2006, pp. 492-499.

[7] Z. Feng, "Wireless sensor networks: a new computing platform for tomorrow's Internet," 2004, pp. I-27 Vol.1.

[8] Ahmed M., Hunag X., Sharma D., “A Taxonomy of Internal Attacks in Wireless Sensor Network”, ICIS 2012, Kuala Lumpur, Malaysia 2012.

[9] Ahmed M., Hunag X., Sharma D., Shutao L., , "Wireless Sensor Network Internal Attacker Identification with Multiple Evidence by Dempster-Shafer Theory.", ICA3PP, Japan 2012.

[10] Ahmed M., Hunag X., Sharma D., Cui H., “Wireless Sensor Network: Characteristics and Architectures”, ICIS 2012 December, Penang, Malaysia 2012.

[11] Ahmed M., Hunag X., Sharma D., “A Novel Framework for Abnormal Behaviour Identification and Detection for Wireless Sensor Networks”, ICIS 2012, Kuala Lumpur, Malaysia 2012.

[12] Shakhnarovish G., Darrell T., Indyk P., “ Nearest-neighbor meathods in learning na d vision”, (MIT press 2005)

[13] Khalaja F., Khalajb M., Khalaj A.H., “Bounded Error for Robust Fault Detection under Uncertainty, Part 1: Proposed Model Using Dempster-Shafer Theory”, Journal of Basic and Applied Scientific Research 2012, 2(2)1233-1240, ISSN 2090-4304 (2012)

[14] Auden J, “ A logic for uncertain Probabilities”, international journal of uncertainity, Fuzziness and Knowledge-Based Systems, Vol. 9, No. 3, June 2001.

[15] Ochirkhand Erdene Ochir, Marine Minier, Fabrice Valois, and Apostolos Kountouris, “Resiliency of Wireless Sensor Networks: Definitions and Analyses”, 2010 17th International Conference on Telecommunications, pp828-835.

[16] Zhang Y, Lee W, “Intrusion Detection in Wireless Ad Hoc Networks”, ACM MOBICOM 2000, Boston, Massachusesttes, USA, pp. 275-283

[17] Silva A. P, Martins M. H, Rocha B. P, Loureiro A. A, Ruiz L. B, Wong H. C, “Decentralized Intrusion Detection In wireless Sensorn Networks”, ACM Q2SWinet 2005, Qubec, Canada, 2005, pp 16-23

[18] S. Marti, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobileadhocnetworks, in: Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom00), 2000, pp. 255–265.

[19] K. Paul, D. Westhoff, Context aware detection of selfish nodes in dsr based ad-hocnetworks, in: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM02), 2002, pp. 178–182.

[20] S. Bansal, M. Baker, Observation-based cooperation enforcement in adhocnetworks, Research Report cs.NI/0307012, 2003.

[21] C. Karlof and D. Wagner, “Secure routing inn wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, Vol. 1 no. 2-3, pp. 293-315, August 2003.

[22] Jing Dong, Reza Curtmola, and Cristina Nita Rotaru, “Parctical Defenses Against Pollution Attacks in Intra-Flow Network Coding for Wireless Mesh Networks,” WiSec’09, March 16-18, 2009, zurich, Switzerland, pp111-122.

[23] D. Charles, K. Jain, and K. Lauter, “Signatures for network coding,” 40th Annual Conference on Information Sciences and Systems, 2006.

[24] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, “An efficient signature-based scheme for securing network coding against pollutions attacks,” in Proc. Of INFOCOM OS , Phoenix, AZ, April, 2008.

[25] M. Krohn, M. Freedman, and D. Mazierres, “On-the-fly verification of rateless erasure codes for efficient content distribution,” Security and Privacy, 2004. Proc. 2004 IEEE Symposium on, pp.226-240, 9-12 May 2004.

[26] C. Gkantsdis and P. Rodriguez, “ Cooperative security for network coding file distribution,” Proc. Of INFOCOM 2006.

[27] Ahmad Ababnah, Balasubramaniam Naatarajan, “Optimal control based strategy for sensor deployment.” IEEE Tran. On Systems, Man, and cybernetics, Part A: Systems and Humans, vol. 41, no. 1 Jan. 2011.

[28] Ahmed Sobeih, Jennifer C Hou, Lu-Chuan Kung, Ning Li, Honghai Zhang, Wei Peng Chen, Hung-Ying Tyan, Sun Yat-Sen and Hyuk Lim, “J-Sim: A simulation and emulation environment for wireless sensor networks,” IEEE Wireless Communications, August 2006, pp104-119.

[29] Y. B. Reddy, “A game theory approach to detect malicious nodes in wireless sensor networks,” Proc. Third International Conference on Sensor Technologies and Applications (SENSORCOMM ’09), 2009, pp. 462-468.

[30] Y. Ma, H. Cao, and J. Ma, “The intrusion detection method based on game theory in wireless sensor network,” Proc. IEEE International Conference on Ubi-Media Computing, 2008, pp. 326-331.

[31] C. Holder, R. Boyles, P. Robinson, S. Raman, and G. Fishel, “Calculating a daily Normal temperature range that reflects daily temperature variability”, American Meteorological Society, June 2006.

[32] W. T. Zhu, Y. Xiang, J. Zhou, R. H. Deng, and F. Bao, “Secure localization with attack detection in wireless sensor networks,” International Journal of Information Security, vol. 10, no. 3, pp. 155-171, 2011.

[33] Y. Zhang, W. Yang, K. Kim, and M. Park, “Inside attacker detection in Hierarchical Wireless Sensor Networks,” in Proc. of the 3rd International conference on innovative computing information and control (ICICIC), 2008.

[34] K. Sentz, “Combination of Evidence in Dempester-Shafer Theory”, System Science and Engineering Department, Binghamton University, SAND 2002-0835, April 2002.

[35] U. Rakowsky, “Fundamentals of the Dempster-Shafer theory and its applications to system safety and reliability modelling” RTA # 3-4, 2007, December – Special Issue.

[36] D. Koks, S. Challa, “An Introduction to Bayesian and Dempster-Shafer Data Fusion” , Published by DSTO Systems Sciences Laboratory, Australia, November 2005.

[37] M. Tabassian, R. Ghaderi, R. Ebrahimpour, “Combination of multiple diverse classifiers using belief functions for handling data with imperfect labels” Expert Systems with Applications 39, Elsevier 2011.

[38] F. Campos, S. Cavalcante, “An Extended Approach for Dempster-Shafer Theory” Information Reuse and Integration, 2003. IRI 2003. IEEE 2003.

**Muhammad Raisuddin Ahmed** currently serves as Lecturer (Teaching Fellow) at the Faculty of Information Sciences and Engineering, University of Canberra (UC), Australia. He was a distinguished member of the Board of directors of ITE&E Canberra Division, Engineers Australia in 2011. Besides, from March 2009 until July 2011, he was working as a Research officer and Project coordinator of BushLAN project at the Plasma research Laboratory, Research School of Physics and Engineering, at the Australian National University (ANU), Australia. During this

time he was also an academic in the College of engineering and computer science at ANU from February 2010 till November 2011. He is pursuing his PhD at the UC, Australia. He has received Master of Engineering studies in Telecommunication and a Masters of Engineering Management degree from the University of Technology, Sydney (UTS), Australia. He obtained his Bachelor of Engineering (Hons) Electronics Majoring in Telecommunications degree from Multimedia University (MMU), Malaysia. His Research interest includes: Wireless Sensor Networks, Distributed Wireless Communication, Blind Source Separation, RF technologies, RFID implementation.

**Xu Huang** has received the B.E. and M.E. degrees and Ph.D. in Electrical Engineering and Optical Engineering prior to 1989 and the second Ph.D. in Experimental Physics in the University of New South Wales, Australia in 1992. He has earned the Graduate Certificate in Higher Education in 2004 at the University of Canberra, Australia. He has been working on the areas of the telecommunications, cognitive radio, networking engineering, wireless communications, optical communications, and digital signal processing more than 30 years. Currently he is the Head of the Engineering at the Faculty of Information Sciences and Engineering, University of Canberra, Australia. He is the Course Conveners “Doctor of Philosophy,” “Masters of Information Sciences (by research),” and “Master of Engineering.” He has been a senior member of IEEE in Electronics and in Computer Society since 1989 and a Fellow of Institution of Engineering Australian (FIEAust), Chartered Professional Engineering (CPEng), a Member of Australian Institute of Physics. He is a member of the Executive Committee of the Australian and New Zealand Association for Engineering Education, a member of Committee of the Institution of Engineering Australia at Canberra Branch. Professor Huang is Committee Panel Member for various IEEE International Conferences such as IEEE IC3PP, IEEE NSS, etc. and he has published about two hundred papers in high level of the IEEE and other Journals and international conference; he has been awarded 9 patents in Australia.

**Hongyan Cui** has received the Ph.D. in School of Telecommunications Engineering in Beijing University of Posts and Telecommunications in 2006. She is engaged in communication network research and development work since 2000. She has been participated in two National 973 Projects, four 863 Projects, two National Nature Funds, a ministerial project, and a corporate-funded research project. She has published over 30 papers in the important journals / conferences, two books since 2003. She applied eight patents. She is the reviewer of the " Chinese Journal of Electronics"," Journal of Communications " ,"Journal of Beijing University of Posts and Telecommunications", "IEEE Networks Magazine SI", "Chaos" etc. She has trained 34 undergraduate students for graduation design,, and guided 31 Masters, in which 16 have graduated , and now she also assisting guided 3 doctoral students. Her research interest is future networks architecture, ESN, and Clustering.